

FILED

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA,
ALEXANDRIA DIVISION

2009 AUG 19 P 4: 26

Project Honey Pot, a dba of Unspam
Technologies, Inc.

Plaintiff,

v.

John Does stealing money from
US businesses through
unauthorized electronic transfers
made possible by computer viruses
transmitted in spam,

Defendants.

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

No. 1:09cv 940
GBL/TRJ

PROJECT HONEY POT'S COMPLAINT FOR VIOLATIONS
OF THE FEDERAL CAN-SPAM ACT

1. Cyber thieves are stealing millions of dollars every month from United States business bank accounts through unauthorized electronic transfers made possible by computer viruses transmitted in spam.

2. Like biological viruses, computer viruses come in different strains that attack a variety of different hosts. Some of the most dangerous computer viruses in broad circulation today are attacking online banking. These strains work in a number of ways, but one key feature is their ability to obtain, through fraud and trickery, the online credentials banks rely upon to identify (i.e., authenticate) their customers during online transactions.

3. Some versions of these viruses contain a keystroke logger function that is capable of capturing every keyboard entry made on an infected machine. By logging keystrokes, the virus can steal a bank customer's username and password, as well as any other "credential"

typed by a user on his or her keyboard. In addition to capturing this critical data, these online bank viruses also use a hidden instant messenger capability to get these short-lived credentials into the hands of their criminal masters in real time.

4. Once the cyber thief has obtained a victim's banking credentials, the real robbery can begin. In the case of a compromised business bank account, the thief will typically exploit the bank account by logging onto the bank's website using the stolen credentials and initiating an automated clearinghouse (or ACH) transfer drawn against the business's bank account.¹ Because many companies pay employees via ACH, these fraudulent transfers are often disguised as a direct deposit payroll to the bank account of a bogus "employee" added to the list of payroll recipients by the thief while he was fraudulently logged into the bank's website using the customer's stolen credentials. In reality, the recipient of the stolen funds is a mere "mule" whose only role is to withdraw the money as soon as it arrives in his account and then hand-carry the cash to a nearby money transfer company storefront to move the funds outside the United States (typically to Russia or Eastern Europe). There, the John Doe defendants retrieve their stolen proceeds from yet more mules who claim the funds from the money services store in the receiving country. The mules on both sides of the transaction are paid a small percentage of the stolen proceeds.

5. The cyber thieves stealing from US business bank accounts depend on a vast network of compromised machines (dubbed "botnets") to provide them the data and resources they need to commit their crimes. These botnets are leased out to illegal businesses that need computer resources they cannot lawfully purchase elsewhere. Increasingly, the

¹ According to the National Automated Clearing House Association (the organization that oversees its operation): "The ACH Network is a processing and delivery system that provides for the distribution and settlement of electronic credits and debits among financial institutions. The ACH Network was developed in response to the astronomical growth of check payments and the many technological advances in the mid-twentieth century and functions as an efficient, electronic alternative to paper checks." See NACHA ACH Rules, at 14 (2009).

monetization of these botnets is the key reason why a vast black market Internet economy is flourishing. Spam is a key revenue source for these botnet operators, as well as a key way to grow the size of the botnet by infecting new machines as they receive spam hiding a virus. Thus, spam plays a critical role in the life cycle of a botnet and botnets are at the core of nearly every cyber threat seen today.

6. On information and belief, the John Doe defendants are initiating thousands of fraudulent ACH transfers every month, in an attempt to steal tens of millions of dollars a month from US businesses. The John Does are focusing their thefts on fraudulent ACH transfers for the same reason Willie Sutton robbed banks decades ago: "That's where the money is." In 2008, NACHA reported over *18.2 billion transactions* were made through ACH, in which nearly *30 trillion dollars* changed hands. See NACHA Press Release, April 6, 2009.²

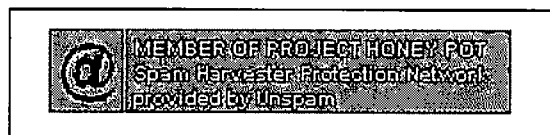
7. On information and belief, despite the vast volume of money moving via ACH, many US-based businesses have a limited understanding of the ACH Network. They do not know much about their rights and responsibilities under the laws that control ACH transactions. Nor do they know very much about the security measures their own banks have in place, let alone the alternative security procedures that are commercially available. As a result, too many US-based businesses are unwittingly putting their money at risk by using online banking to initiate ACH transfers.

8. If there were ever any doubt, today it is clear the key to stopping cyber threats is to identify those responsible for it, and those who are enabling it – either knowingly or unknowingly, and getting that information into the hands of those willing and able to do something about it.

² <[http://www.nacha.org/news/news/pressreleases/2009/2008%20ACH%20Stats%20\(Final\).pdf](http://www.nacha.org/news/news/pressreleases/2009/2008%20ACH%20Stats%20(Final).pdf)>.

9. Discovering the identity of those behind today's cyber threats is not simple, but it is not impossible either. For example, to hide successfully, spammers have to do more than just avoid putting their name in their messages. Everything they do has to be anonymous; they have to hide while simultaneously fooling their victims (and nearly everyone else who is providing them with some service essential to their criminal enterprise) into thinking they are running a legitimate business.

10. The first thing a spammer needs is a long list of email addresses to spam. Spammers get email addresses in two primary ways. They steal them (via harvesting) or they guess them (via dictionary attacks). The most common way spammers steal email addresses is by harvesting them from websites, using web spiders. This makes life difficult for the rest of us because posting email addresses on a website is a convenient way to facilitate communications between visitors to a website and the owners of the website. Owners of websites who want to display email addresses can obtain some protection from harvesters by installing a Project Honey Pot on their website, and displaying this Project Honey Pot logo on their website:³



The logo serves as a warning to harvesters that all of the email addresses displayed anywhere on the website are protected by Project Honey Pot and deters harvesters by putting them at legal risk if they spam any addresses harvested from the website.

³ The website for the logo can be found at http://www.projecthoneypot.org/how_to_avoid_spambots_5.php.

11. Domain name owners who want to protect their email system from spam can obtain some protection by donating an MX record to Project Honey Pot, and then publicly disclosing the fact of their donation (but they should not disclose the specific MX record donated, as spammers will simply avoid this MX record and continue to send spam to MX records not donated to PHP). By publicly disclosing their affiliation with Project Honey Pot, PHP members warn spammers that their domain names are protected by Project Honey Pot.

Project Honey Pot, a dba of Unspam Technologies, Inc.

12. Project Honey Pot (www.projecthoneypot.org) is a distributed network of spam-tracking honey pots. The project allows spammers, phishers, and other e-criminals to be tracked throughout the entire "spam cycle." On information and belief, Project Honey Pot was the first distributed e-mail harvesting research effort linking those that gather e-mail addresses by scraping websites with those that send unsolicited and frequently fraudulent messages. More than 60,000 users from at least 165 countries actively participate in Project Honey Pot's effort to track and stop cyber crime. Project Honey Pot was created by Unspam Technologies, Inc (www.unspam.com) – an anti-spam company with the singular mission of helping design and enforce effective anti-spam laws. Unspam Technologies, Inc. is a Delaware corporation.

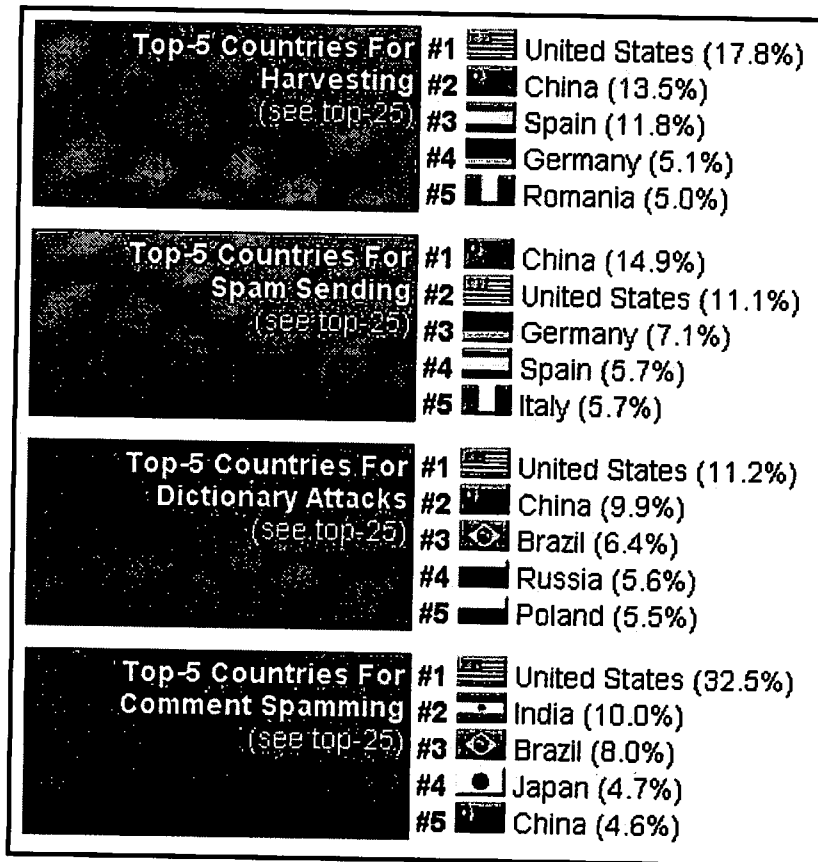
13. Project Honey Pot receives MX record donations from the owners of Internet domain names. Through those donations, email messages addressed to any username hosted at a donated domain name are directed to email servers owned and maintained by Project Honey Pot, and those email messages are then processed by and stored on computer equipment owned and maintained by Project Honey Pot. Project Honey Pot also makes available to Internet website owners email address honey pots that can be installed on their webpages. When a harvester visits those webpages looking for email addresses to steal, the harvester is handed a

unique email address hosted within Project Honey Pot's distributed network of donated MX records. The harvester's IP address, the date and time of the visit and other characteristics of the harvester are recorded by Project Honey Pot and maintained for analysis and tracking. When a spam message is received thereafter at the unique email address, Project Honey Pot can tie the spam message (and the spammer) to the harvester that was given that email address.

14. Project Honey Pot is currently monitoring over 41 million honey pot email addresses. Between January 2005 and August 2009, John Doe spammers transmitted over 825 million spam messages to hundreds of thousands of unique email addresses belonging to PHP members who have donated an MX record to, and are receiving anti-spam protection from, Project Honey Pot. All of these email addresses were illegally harvested by the spammer (or one of his co-conspirators) from a website hosting a PHP honey pot, or were the subject of dictionary spam attacks that indiscriminately targeted random usernames hosted within Internet domain names that have donated an MX record to, and are receiving anti-spam protection from, Project Honey Pot.

15. Through August 2009, Project Honey Pot has identified over 57 million unique spam server IP addresses, 72 thousand unique harvester IP addresses, 7.6 million unique dictionary attack spam server IP addresses, and from April 2007 through April 2009, has identified 244 thousand comment spam server IP addresses. Contrary to the popular belief that most cyber criminals are beyond the reach of the United States, Project Honey Pot's data indicates many of the John Doe Defendants in this case heavily depend on their ability to gain access to IP addresses that are located within the United States. The United States ranks #1 in three of the four aggregate IP-address categories tracked and reported publicly by Project Honey

Pot -- and nearly one-third of all comment spammers launch their illegal spam from a U.S.-based IP address:



16. Many of the spam messages Project Honey Pot receives contain online bank viruses designed to attack online banking by stealing the credentials used by banks to authenticate their customers. For example, on information and belief, common strains of the online banking viruses in circulation today are distributed in spam masquerading as an update to a popular email program. Victims fooled by the ruse who click on the link in the spam, however, infect their computer and thereafter give their online banking credentials (and then their money) to the John Doe defendants. In June 2009 alone, Project Honey Pot received over 237,000 spam email messages masquerading as this bogus email update file.

17. Every email spam message transmitted to a Project Honey Pot honey pot harms Project Honey Pot. Each message is received by a computer server controlled by and paid

for by Project Honey Pot, which then must process, store and analyze the message to help protect the website owners who have installed honey pots on their webpages from harvesters and comment spammers, and to protect the domain name owners who have donated MX records from email spam attacks.

18. By this action, Plaintiff seeks: (i) an injunction to prevent further unlawful conduct; (ii) compensatory damages; (iii) punitive damages; (iv) attorneys' fees and costs of suit.

John Doe Defendants

19. Defendants' identity is currently unknown to Plaintiff because Defendants have intentionally acted to hide their identity to evade detection. They are systematically transmitting spam messages that contain computer viruses designed to steal online banking credentials from unsuspecting computer users, and are using those credentials to steal millions of dollars a month from US-based businesses through unauthorized electronic transfers from those businesses' bank accounts.

JURISDICTION AND VENUE

20. This action arises out of Defendants' violation of the Federal CAN-SPAM Act. The Court has subject matter jurisdiction of this action based on 28 U.S.C. § 1331.

21. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Plaintiff's claims, together with a substantial part of the property that is the subject of Plaintiff's claims, are situated in this judicial district. For example, as of November 2008, 832 PHP members self-report they are located in Virginia. PHP members have installed honey pots on 349 websites that are located in Virginia, and these Virginia-based honey pots have distributed 73,794 email addresses to identified

harvesters world-wide. In addition to PHP's substantial presence in Virginia, the spammers also have substantial connections to Virginia. For example, as of November 2008, the spammers have used 217 harvester IP addresses in Virginia to harvest 9,608 PHP member honey pot email addresses. The spammers have also used 77,629 spam server IPs located in Virginia to transmit 803,519 spam messages to PHP member honey pot email addresses. And on 1,232 occasions, spammers have relied entirely on Virginia IP addresses to further their illegal enterprise – by harvesting a PHP member email address from a Virginia-based IP address and then sending spam to that address from a spam server using a Virginia-based IP address. In addition, the webpages advertised in the spam messages were all visible in Virginia.

22. The federal District Court for the Eastern District of Virginia has personal jurisdiction over Defendants based on the following facts: Defendants initiated emails from the Eastern District of Virginia, gained unauthorized access to computer servers located in the Eastern District, caused tortious injury in the Eastern District, and conducted business in the Eastern District of Virginia.

COUNT I

Violation of the Federal CAN-SPAM Act (15 U.S.C. § 7701 et seq.)

23. Plaintiff repeats and re-alleges the allegations preceding this paragraph.

24. Defendants initiated the transmission, to a protected computer, of a commercial electronic mail message that contained, or was accompanied by, header information that was materially false or materially misleading, in violation of 15 USC § 7704(a)(1).

25. In a pattern or practice, Defendants initiated the transmission to a protected computer of a commercial electronic mail message that did not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient could use to submit, in a manner specified in the message, a reply

electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received, in violation of 15 USC § 7704(a)(3).

26. In a pattern or practice, Defendants initiated the transmission of a commercial electronic mail message to a protected computer and failed to provide: (i) clear and conspicuous identification that the message was an advertisement or solicitation; (ii) clear and conspicuous notice that the recipient could decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender, in violation of 15 USC § 7704(a)(5).

27. Plaintiff is an Internet access service adversely affected by the above violations, and is entitled to an injunction barring further violations, statutory damages of \$100 for every attempted transmission of a spam message that contains false or misleading transmission information, statutory damages of \$25 for every attempted transmission of a spam message that otherwise fails to comply with the Federal CAN-SPAM Act, treble damages resulting from Defendants' use of email harvesters and dictionary attacks to facilitate their violations of the CAN-SPAM Act, and attorney fees and costs, as authorized by 15 USC § 7706(g).

PRAYER FOR RELIEF

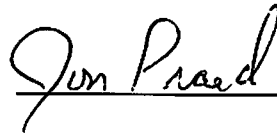
WHEREFORE, Plaintiff requests entry of judgment in its favor and against Defendants:

1. Granting preliminary and permanent injunctive relief against Defendants, and all those in privity or acting in concert with Defendants, enjoining them from directly or indirectly violating the terms of the CAN-SPAM Act;

2. Awarding Plaintiff compensatory and punitive damages in an amount to be proven at trial;
3. Awarding Plaintiff attorneys' fees and costs associated with prosecuting this action; and
4. Granting Plaintiff such other or additional relief as this Court deems just and proper under the circumstances.

Dated: August 18, 2009

Respectfully submitted,

A handwritten signature in cursive script, reading "Jon Praed", written over a horizontal line.

INTERNET LAW GROUP

Jon L. Praed (VSB #40678)
4121 Wilson Boulevard, Suite 101
Arlington, Virginia 22203
(703) 243-8100

*Attorneys for Plaintiff Project Honey Pot,
a dba of Unspam Technologies, Inc.*